UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,694	09/29/2000	Manav Mishra	42390P9326	1491

7590 12/22/2005

Libby N Ho
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
LAZARO, DAVID R	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 12/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/675,694	MISHRA ET AL.	
	Examiner	Art Unit	
	David Lazaro	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *30-52 and 54-73* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *30-52 and 54-73* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the RCE filed 10/03/2005.

2. Claims 30, 34, 38, 39, 43, 44, 46, 48, 49, 50, 56, 57, 59, 60, 64, 70 and 72 were amended.

3. Claims 1-29 and 53 are canceled.

4. Claims 30-52 and 54-73 are pending in this office action.

Response to Amendment

5. Applicant's arguments filed 10/03/2005 have been fully considered but they are not persuasive. See Response to Arguments. Therefore, the previous grounds of rejection, as presented in the office action mailed 05/03/2005, are respectfully maintained.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 30-52 and 54-73 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,772,333 by Brendel (Brendel).

8. With respect to Claim 39, Brendel teaches a method comprising:

receiving a user request corresponding to a transaction at a dispatcher (Col. 9 lines 29-36), the user request comprising a session identifier (ID) (Col. 9 lines 57-65);

determining if the transaction is a secure transaction (Col. 9 lines 57-63);

determining if the session ID exists in a mapping table at the dispatcher (Col. 9 lines 1-12), if the transaction is a secure transaction (Col. 9 lines 63-67), the mapping table being maintained by the dispatcher (Col. 9 lines 1-12); and

assigning a server to the user request at the dispatcher (Col. 10 lines 5-17) and creating a secure tunnel between the dispatcher and the user at the dispatcher if the transaction is a secure transaction and if the session ID does not exist in the mapping table (Col. 10 lines 5-17 - Note: The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

9. With respect to Claim 30, Brendel teaches all the limitations of Claim 34 and further teaches wherein creating a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers (Col. 10 lines 5-17 and Col. 2 lines 9-26 - Note: the secure tunnels are established as data is already being encrypted.).

10. With respect to Claim 31, Brendel teaches all the limitations of Claim 34 and further teaches the secure tunnel comprises a secure sockets layer (SSL) context (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

11. With respect to Claim 32, Brendel teaches all the limitations of Claim 31, and further teaches the SSL context comprises a source address, a destination address and an encryption algorithm (Col. 3 line 58 - Col. 4 line 25).

12. With respect to Claim 33, Brendel teaches all the limitations of Claim 39 and further teaches using a load balancing algorithm to assign a server to the user request if the transaction is not a secure transaction (Col. 9 lines 29-56).

13. With respect to Clam 34, Brendel teaches all the limitations of Claim 39 and further teaches subsequently receiving a second request comprising the session 1D; selecting the server corresponding to the session ID using the mapping table (Col. 9 line 63 - Col. 10 line 17); and sending the second request to the selected server (Col. 10 lines 5-17).

14. With respect to Claim 35, Brendel teaches all the limitations of Claim 39 and further teaches wherein determining if the transaction is a secure transaction comprises determining if an SSL packet is associated with the request (Col. 9 lines 57-63).

15. With respect to Claim 36, Brendel teaches all the limitations of Claim 39 and further teaches wherein a secure transaction comprises transactions in which information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58).

16. With respect to Claim 37, Brendel teaches all the limitations of Claim 39 and further teaches wherein a secure transaction comprises transactions in which personal data and credit card information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58)

17. With respect to Claim 38, Brendel teaches all the limitations of Claim 39 and further teaches receiving a second request comprising a second session ID (Col. 10 lines 5-17); selecting the server corresponding to the first session ID using the mapping table (Col. 10 lines 5-17); sending the second request to the selected server (Col. 10 lines 5-17); and applying a quality of service algorithm to prioritize the first request and the second request (Col. 14 lines 11-18).

18. With respect to Claim 40, Brendel teaches all the limitations of Claim 39 and further teaches using a load balancing algorithm to assign the server to the user request (Col. 10 lines 5-17).

19. With respect to Claim 41, Brendel teaches all the limitations of Claim 39 and further teaches sending the request to a server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 lines 63 - Col. 10 line 4).

20. With respect to Claim 42, Brendel teaches all the limitations of Claim 39 and further teaches adding the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

21. With respect to Claim 43, Brendel teaches all the limitations of Claim 39 and further teaches wherein creating a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers (Col. 10 lines 5-17 and Col. 2 lines 9-26).

22. With respect to Claim 44, Brendel teaches all the limitations of Claim 43 and further teaches creating the secure tunnel comprises creating a secure sockets layer (SSL) context having a source address, a destination address and an encryption algorithm (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

23. With respect to Claim 45, Brendel teaches all the limitations of Claim 39 and further teaches wherein determining if the transaction is a secure transaction comprises determining if an SSL packet is associated with the request (Col. 9 lines 57-63).

24. With respect to Claim 46, Brendel teaches 46 a method comprising:

receiving a user request corresponding to a transaction at a dispatcher (Col. 9 lines 29-37), the user request comprising a session identifier (ID) (Col. 9 lines 57-65);

assigning a server to the user request at the dispatcher (Col. 10 lines 5-17);

determining if the transaction is a secure transaction (Col. 9 lines 57-63);

creating a secure tunnel between the dispatcher and the user at the dispatcher if the transaction is a secure transaction (Col. 10 lines 5-17);

adding the session ID, the server assignment, and the secure tunnel assignment as an entry to a mapping table at the dispatcher if the transaction is a secure transaction (Col. 10 lines 5-17 - The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

25. With respect to Claim 47, Brendel teaches all the limitations of Claim 46 and further teaches determining if the session ID exists in the mapping table, if the

transaction is a secure transaction and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 4).

26. With respect to Claim 48, Brendel teaches all the limitations of Claim 46 and further teaches wherein creating a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers (Col. 10 lines 5-17 and Col. 2 lines 9-26).

27. With respect to Claim 49, Brendel teaches all the limitations of Claim 46 and further teaches creating the secure tunnel comprises creating a secure sockets layer (SSL) context having a source address, a destination address and an encryption algorithm (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

28. With respect to Claim 50, Brendel teaches all the limitations of Claim 46 and further teaches subsequently receiving a second request comprising the session ID; determining if the session ID exists in the mapping table maintained by the dispatcher (Col. 9 lines 1-12); and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 17).

29. With respect to Claim 51, Brendel teaches all the limitations of Claim 46 and further teaches wherein a secure transaction comprises transactions in which information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58).

30. With respect to Claim 52, Brendel teaches all the limitations of Claim 46 and further teaches receiving a second request comprising a second session ID (Col. 10 lines 5-17); selecting the server corresponding to the first session ID (Col. 10 lines 5-17); sending the second request to the selected server (Col. 10 lines 5-17); and applying a quality of service algorithm to prioritize the first request and the second request (Col. 14 lines 11-18).

31. With respect to Claim 57, Brendel teaches an article of manufacture including a machine-readable medium having stored thereon data representing sequences of instructions, which, when executed by a machine, cause the machine to perform operations including:

receiving a user request corresponding to a transaction at a dispatcher (Col. 9 lines 29-36), the user request comprising a session identifier (ID) (Col. 9 lines 57-65);

determining if the transaction is a secure transaction (Col. 9 lines 57-63);

determining if the session ID exists in a mapping table at the dispatcher (Col. 9 lines 1-12), if the transaction is a secure transaction (Col. 9 lines 63-67) the mapping table being maintained by the dispatcher (Col. 9 lines 1-12); and

assigning a server to the user request at the dispatcher and creating a secure tunnel between the dispatcher and the user at the dispatcher if the transaction is a secure transaction and if the session ID does not exist in the mapping table (Col. 10 lines 5-17 - Note: The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the

assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

32. With respect to Claim 54, Brendel teaches all the limitations of Claim 57 and further teaches using a load balancing algorithm to assign a server to the user request if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5 - 17).

33. With respect to Claim 55, Brendel teaches all the limitations of Claim 57 and further teaches adding the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

34. With respect to Claim 56, Brendel teaches all the limitations of Claim 57 and further teaches creating a secure tunnel comprises selecting from among a plurality of established secure tunnels with a plurality of servers, assigning a secure tunnel to the assigned server, and adding as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17 and Col. 2 lines 9-26).

35. With respect to Claim 58, Brendel teaches all the limitations of Claim 57 and further teaches sending the request to a server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 lines 63 - Col. 10 line 4).

36. With respect to Claim 59, Brendel teaches all the limitations of Claim 57 and further teaches creating the secure tunnel comprises creating a secure sockets layer

(SSL) context having a source address, a destination address and an encryption algorithm (Col. 10 lines 5-17 and Col. 3 line 58 - Col. 4 line 25).

37. With respect to Claim 60, Brendel teaches an article of manufacture including a machine-readable medium having stored thereon data representing sequences of instructions, which, when executed by a machine, cause the machine to perform operations including:

receiving a user request corresponding to a transaction at a dispatcher (Col. 9 lines 29-37), the user request comprising a session identifier (ID) (Col. 9 lines 57-65);

assigning a server to the user request at the dispatcher(Col. 10 lines 5-17);

determining if the transaction is a secure transaction (Col. 9 lines 57-63);

creating a secure tunnel between the dispatcher and the user at the dispatcher if the transaction is a secure transaction (Col. 10 lines 5-17);

adding the session ID, the server assignment, and the secure tunnel assignment as an entry to a mapping table at the dispatcher if the transaction is a secure transaction (Col. 10 lines 5-17 - The examiner broadly interprets a tunnel to be a designated channel of communication based on the specification on page 6, line 26. The connection to the assigned server is a designated channel of communication and communications are encrypted when the transaction is secure, hence a secure tunnel).

38. With respect to Claim 61, Brendel teaches all the limitations of Claim 60 and further teaches determining if the session ID exists in the mapping table, if the transaction is a secure transaction and sending the request to the server corresponding

to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 4).

39. With respect to Claim 62, Brendel teaches all the limitations of Claim 60 and further teaches subsequently receiving a second request comprising the session ID; determining if the session ID exists in the mapping table; and sending the request to the server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 9 line 63 - Col. 10 line 17).

40. With respect to Claim 63, Brendel teaches all the limitations of Claim 60 and further teaches receiving a second request comprising a second session ID (Col. 10 lines 5-17); selecting the server corresponding to the first session ID (Col. 10 lines 5-17); sending the second request to the selected server (Col. 10 lines 5-17); and applying a quality of service algorithm to prioritize the first request and the second request (Col. 14 lines 11-18).

41. With respect to Claim 64, Brendel teaches a system comprising:

a mapping table at a dispatcher, maintained by the dispatcher (Col. 9 lines 1-12) and containing session identifiers (IDs) linked to server and secure tunnel assignments (Col. 9 line 63 - Col. 10 line 17); and

the dispatcher to receive a user request corresponding to a transaction (Col. 9 lines 29-36), the user request comprising a session ID (Col. 9 lines 57-65), to determine if the transaction is a secure transaction (Col. 9 lines 57-63), to determine if the session ID exists in the mapping table, if the transaction is a secure transaction(Col. 9 line 63 -

Col. 10 line 17), and to send the request to a server corresponding to the session ID in the mapping table, if the session ID exists in the mapping table (Col. 10 line 5-17).

42. With respect to Claim 65, Brendel teaches all the limitations of Claim 64 and further teaches a load balancing table and wherein the dispatcher assigns a server to the user request using the load balancing table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

43. With respect to Claim 66, Brendel teaches all the limitations of Claim 65 and further teaches the dispatcher adds the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 line 5-17).

44. With respect to Clam 67, Brendel teaches all the limitations of Claim 65 and further teaches the dispatcher determines if the transaction is a secure transaction by determining if an SSL packet is associated with the request (Col. 9 lines 57-63).

45. With respect to Claim 68, Brendel teaches all the limitations of Claim 67 and further teaches a secure transaction comprises transactions in which information about the user is saved at the assigned server (Col. 10 lines 31-36 and Col. 11 lines 46-58)

46. With respect to Claim 69, Brendel teaches all the limitations of Claim 65 and further teaches a quality of service (QoS) manager in communication with the dispatcher to decide which one of multiple user requests is processed if multiple user requests are sent to the same server (Col. 14 lines 11-18).

47. With respect to Claim 70, Brendel teaches a system comprising:

a load balancing table (Col. 10 lines 5-17);

a mapping table at a dispatcher, maintained by the dispatcher (Col. 9 lines 1-12) and containing session identifiers (IDs) linked to server and secure tunnel assignments (Col. 9 line 63 - Col. 10 line 17); and

the dispatcher to receive a user request corresponding to a transaction (Col. 9 lines 29-36), the user request comprising a session ID (Col. 9 lines 57-65), to determine if the transaction is a secure transaction (Col. 9 lines 57-63), to determine if the session ID exists in the mapping table, if the transaction is a secure transaction (Col. 9 line 63 - Col. 10 line 17), to assign a server to the user request using the load balancing table and to create a secure tunnel to the assigned server if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

48. With respect to Claim 71, Brendel teaches all the limitations of Claim 70 and further teaches the dispatcher further assigns a server to the user request using the load balancing table if the transaction is not a secure transaction (Col. 9 lines 37-56).

49. With respect to Claim 72, Brendel teaches all the limitations of Claim 70 and further teaches the dispatcher creates the secure tunnel by selecting from among a plurality of established secure tunnels with a plurality of established servers, if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17 and Col. 2 lines 9-26).

50. With respect to Claim 73, Brendel teaches all the limitations of Claim 70 and further teaches the dispatcher further adds the session ID and the server assignment as an entry to the mapping table if the transaction is a secure transaction and the session ID does not exist in the mapping table (Col. 10 lines 5-17).

Response to Arguments

51. Applicants' arguments filed 10/03/2005 have been fully considered but they are not persuasive.

52. Applicants comment on page 12 of the remarks - "*The key comments from the Examiner would appear to be: ...2) "The claim language does not state any limitations in regards to how and where the session ID is generated nor any relationship between the generation of the session ID and assignment of a secure tunnel." Applicants have attempted to address these comments by the Examiner in the amendments above.*"

a. Examiner's response - To further clarify this comment, the examiner refers to applicants' specification. From page 4, lines 9-16, and page 7, lines 3-9, it appears that the session ID is generated based on an initial login interaction with the dispatcher, particularly the creation of a secure SSL connection between the client and the dispatcher. The session ID generated from the creation of this SSL connection is subsequently mapped to an SSL context that corresponds to previously existing SSL tunnel and corresponding SSL context between the dispatcher and a selected server. Essentially, there may be two or more SSL contexts; one between the client and the dispatcher and one between the dispatcher and a selected server and any additional servers. Since there is more than one SSL context, it is importance to realize that the session ID of concern (i.e., the one being mapped) is associated with the SSL context between the client and the dispatcher. The examiner's comment from the advisory action (07/19/2005) was noting that the claims did not state limitations that clarify this subject matter. The examiner feels the currently pending claims still do not fully clarify this subject matter. The examiner suggests that any future amendments

should distinguish between the SSL context between the client and the dispatcher and the SSL context between the dispatcher and the selected server and should further clarify that the session ID being mapped, directly corresponds to the SSL context between the client and dispatcher. The examiner is open to any discussions regarding purposed amendments.

53. Applicants argue on page 12 of the remarks - "*The key comments from the Examiner would appear to be: 1) "The examiner does not see how the 'lookup table' of Brendel is any different from the mapping table of applicants' invention." Referring to Claim 39, the lookup table of Brendel is different from the mapping table in that the mapping table is located at and maintained by the dispatcher, not the server. Claim 39 has been amended to so state.*"

b. Examiner's response - Brendel does not state that the mapping table is located on the server. Col. 9, lines 2-3, explicitly states, "FIG. 7 shows a table in the load-balancer that assigns the server based on the SSL session ID." As such, it is clear that the mapping table is "at the dispatcher" and "maintained by the dispatcher" as indicated in the claim language.

Conclusion

54. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

55. U.S. Patent 6,367,009 by Davis et al. "Extending SSL to a multi-tier environment using delegation of authentication and authority" April 2, 2002. Discloses a client to middle tier SSL connection where the middle tier establishes a SSL connection to the end tier on behalf of the client.

56. U.S. Patent 6,732,269 by Baskey et al. "Methods, systems and computer program products for enhanced security identity utilizing an SSL proxy" May 4, 2004. Discloses an SSL proxy for forwarding multiple client SSL connections through a persistent SSL connection to a transaction server.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Lazaro whose telephone number is 571-272-3986. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

David Lazaro
December 19, 2005

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER